A Study on Improve Share Image of Visual Cryptography

沈友硯、陳文儉,吳昭明

E-mail: 9606935@mail.dyu.edu.tw

ABSTRACT

The visual cryptography（VC） was developed by M. Naor and A. Shamir in 1994. It shares the secret among participants and transmits the parts of secret separately. The secret can only be decrypted by all participants of a qualified set. The most notable feature of visual cry- ptography is that it can recover a secret image without any computation and any cryptography knowledge. It just uses the characteristics of human vision to decrypt encrypted images. For the simplest visual cryptography scheme, the secret image with size n×n is encrypted into two share images. Both of the share images are with the same size 2n×2n. Therefore, total data quantity and storage space are 8 times of the secret image. To decrypt the secret, the share images are printed on transparencies first and then stack them together. In this thesis, we do an improvement on share image of visual cryptography. In traditional VC, the two share images are with the same size. The share image is four times as large as the secret image. Utilize the symmetric property of 90° rotation for square image, one of the share can be reduced to 1/4 of the original. So, the two share images produced by the proposed new scheme are with different sizes. These two shares can be seen as the cipher text and the secret key in the cryptographic system. During decoding, you need to stack the smaller share with the four corners （top-left,top-right, bottom-left, bottom -right）of the larger share, separately. For each stacking, one quarter of the secret image will be revealed. In summary, the proposed VC method not only protects the secret image but also reduces the size of one share image into 1/4. Therefore, data quantity and storage space is less than the traditional VC.

Keywords : Visual Cryptography（VC）, Secret Image, Share Image

Table of Contents

REFERENCES

[1] N. Naor and A. Shamir,“ Visual cryptography, advances in cryptography ”, Eurocrypt ’ 94, Lecture Note in Computer Science Springer-Verlag, Perugia, Italy, pp.1-12, 1994.

[2] Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson,“ Extended Schemes for Visual Cryptography ”, Theoretical Computer Science, 1996.

[3] L.H. Chen, C.C. Wu,“ A Study on Visual Cryptography ”, Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[4] C.S. Tsai, C.C. Chang, and T.S. Chen,“ Sharing multiple secrets in digital images ”, Journal of Systems and Software, Vol. 64, pp. 163-170, 2002.

[5] H.C. Wu, C.C. Chang,“ Sharing visual multi-secrets using circle shares ”, Computer Standards & Interfaces, Vol. 28, 2005, pp. 123-135, 2005.

[6] A. Houmansadr, S. Ghaemmaghami.“ A Novel Video Watermarking Method Using Visual Cryptography ”, Engineering of Intelligent Systems, 2006 IEEE International Conference on Publication Date: 22-23 April 2006. pp. 1-5, 2006.

[7] Hyoung Joong Kim, Yongsoo Choi, ” A New Visual Cryptography Using Natural Images “ , Circuits and Systems, ISCAS 2005. IEEE International Symposium on 23-26 May 2005 pp. 5537-5540, Vol. 6. 2005.

[8] D.j. Wang, L.G. Jiang, G.R. Feng,“ Novel blind non-additive robust watermarking using 1-D chaotic map ”, Acoustics, Speech, and Signal Processing, 2004. Proceedings. （ICASSP '04）. IEEE International Conference on Publication Date: 17-21 May 2004 Volume: 3, pp. iii- 417-20

vol.3, 2004.
[9] Wong P., Memon N.,“ Secret and public key image watermarking schemes for image authentication and ownership verification ”, IEEE Transactions on Image Processing, 2001, pp. 1593-1601, 2001.
[10] Chang, C. C., Chuang, J. C. and Lin, P. Y.,“ Sharing a Secret Two-Tone Image in Two Gray-Level Images ”, Proceedings of The First International Workshop on Security in Networks and Distributed Systems, pp. 300-304, Jul. 2005.
[11] Hou, Y. C., Chang, Chao-Yuan, and Tu, S. F. （2001.07）,“ Visual Cryptography for Color Images Based on Halftone Technology ”, Proceedings of SCI 2001/ISAS 2001, Vol. XIII, Orlando, Florida. pp. 441-445, 2001.
[12] C. C. Lin, W. H. Tsai,“ Visual cryptography for gray-level images by dithering techniques ”, Pattern Recognition Letters Vol. 24, pp. 349-358, 2003.
[13] W.-Q. Yan, D. Jin, and M. S. Kankanhalli,“ Visual cryptography for print and scan applications ”, Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium, vol. 5, pp. 572-575, 2004.